Association for Progressive Communications submission to the UN Working Group on Business and Human Rights on the issue of procurement and deployment of AI systems by states and business enterprises

This submission aims to provide input for the drafting of the report “The Use of Artificial Intelligence and the UN Guiding Principles on Business and Human Rights”, to be prepared by the UN Working Group on the issue of human rights and transnational corporations and other business enterprises for presentation to the UN Human Rights Council. It addresses the “questions for other stakeholders” as per the call for inputs made available by the Office of the United Nations High Commissioner for Human Rights (OHCHR).

ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

JANUARY 2025

1. What do you consider are the main human rights risks linked to the procurement and deployment of AI systems by states and in which area?

The procurement and deployment of artificial intelligence (AI) systems by states presents significant human rights risks, particularly affecting marginalised communities and individuals. These risks include the perpetuation and deepening of existing discriminatory practices and the replication of data gaps through automated decision-making systems in public services, social welfare and law enforcement; infringements of privacy and data protection are also important threats.

The processes to develop AI governance, as much as to develop technical implementations, may lead to further human rights risks if intersectional impact assessments are not duly undertaken, and if the rights holders are not involved, through consultation and active participation.

The procurement of AI applications by states also calls for a careful cost/benefit analysis that requires a critical assessment concerning the public goals sought and the high investments required. This is especially important in view of the risk of tech dependency and challenges imposed by the privatisation of infrastructure for AI systems used in (often critical) public services. The increasing reliance on AI systems for public services creates a concerning pattern of technological dependency that poses significant human rights risks, particularly when the underlying digital infrastructure and technical expertise remain concentrated in the hands of a few private technology companies. This concentration of power creates multiple layers of vulnerability: economic distortions arise from monopolistic pricing and vendor lock-in situations; information asymmetries develop when government agencies lack the technical capacity to fully understand or audit the systems they deploy; infrastructure dependencies emerge when essential public services become reliant on proprietary systems; and communication channels between citizens and government become mediated by private technological interfaces. The development of public interest AI and public digital infrastructure becomes crucial not only for ensuring democratic control over these systems, but also for guaranteeing that public services remain accessible, adaptable and accountable to all citizens. Without such public capacity, states risk compromising their ability to independently assess, modify or replace AI systems when they fail to serve the public interest, potentially leaving vulnerable populations at the mercy of profit-driven technological solutions that may not prioritise their needs or rights.

The **lack of transparency** in procurement processes further compounds these issues. It is important to ensure that information is accessible and understandable to the general public, so that public oversight can take place. Techno jargon should be avoided and the transparency of algorithms and models used should be a requirement. Shortcomings in relation to the explainability of AI systems can negatively impact public trust and endanger compliance.

The case of the emergency aid programme deployed in Brazil as part of the COVID-19 response policy, which was analysed by one of APC's members,[1] is an example that wraps these risks together:

- Regarding **discriminatory practices**, the implementation of AI systems in public services reveals deep-rooted concerns about the perpetuation of discriminatory practices through automated decision making. As evidenced in Brazil's emergency aid programme, these systems often embed and amplify historical biases, disproportionately impacting women, gender-diverse individuals, racial and ethnic minorities, and persons with disabilities.
- The replication of **data gaps** through these systems was particularly troubling, as existing datasets frequently fail to represent society's full diversity, leading to solutions that catered primarily to dominant groups while ignoring the specific needs and circumstances of marginalised populations.
- Regarding **privacy concerns**, inadequate data protection measures created significant risks of surveillance and data leakage.
- Regarding **tech dependency and the privatisation of infrastructure for AI systems** used in critical public services, the implementation relied heavily on specific technological platforms and private sector partnerships, creating barriers to access and accountability.

[1] Tavares, C., Fonteles, J., Simão, B., & Valente, M. (2022). *O Auxílio Emergencial no Brasil: Desafios na implementação de uma política de proteção social datificada*. Derechos Digitales. https://derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf

- The **absence of meaningful participation from affected communities** in system selection and implementation, coupled with insufficient needs assessments, often results in AI solutions being deployed where simpler alternatives might be more appropriate; the centralised implementation of Brazil's emergency aid programme illustrates how the lack of local input and consideration of diverse needs can create significant barriers to access, particularly for marginalised communities. This situation was exacerbated by increasing technological dependency and the concentration of power in the hands of a few tech companies, creating concerning implications for the delivery of critical public services.
- Additionally, the problems derived from **lack of robust accountability regimes** was evidenced in the experience of Brazil's emergency aid programme, where judicial action often became the only recourse for challenging incorrect determinations, highlighting the urgent need for more accessible and effective accountability measures.

Finally, the impact derived from the environmental footprint of AI servers, especially generative AI, must be analysed as a human rights risk. This **environmental impact** is not only directly linked to the harms of excessive energy consumption on ecosystems and waste management, but also concerns the loose regulations and lack of corporate transparency about this data, including disclosing what population segments will be affected the most, and who is to absorb and be accountable for the costs of these impacts.

2. What do you consider are the main human rights risks linked to the procurement and deployment of AI systems by business enterprises outside the technology sector in their operations, products and services and in which area?

In the private sector, the primary risks emerge from the uncritical adoption of AI systems without adequate consideration of the actual need for them and their intersectional impacts. Businesses outside the technology sector often deploy AI systems for recruitment, performance monitoring and customer service without understanding their discriminatory effects on workers and consumers from marginalised communities. These systems frequently perpetuate gender, racial and socioeconomic inequalities while creating new forms of digital exclusion. Of particular concern is the deployment of AI in essential services like healthcare and financial services, where biased algorithms can significantly impact access to critical resources.

In healthcare, biases in AI may not reflect the patient base, impacting diagnostics and treatment routes. Credit scoring can limit people’s access to financial services and violate privacy, often with disproportionate effects on marginalised groups. In labour, AI applications may lead to undue surveillance of workers and their deployment may negatively impact employment in low-skill sectors. Automation in advertising and customer engagement may allow exploitation of consumer vulnerabilities and monetise the expropriation of behavioural data.

3. Are there any policies, regulations or frameworks taken at the national, regional and international levels to address the human rights risks linked to the procurement and/or deployment of AI by states? Please provide examples. What are the main opportunities to adopt and/or strengthen these frameworks?

- The Beijing review processes (both at regional and international levels), particularly Beijing+25 and the ongoing Beijing+30 preparations, have increasingly highlighted the gendered impacts of AI systems and automated decision making. These reviews have emphasised how AI procurement and deployment by states can perpetuate gender biases and discrimination, calling for human rights impact assessments that specifically consider gender implications. The Beijing Platform for Action's framework, while pre-dating modern AI, has evolved to address technological developments that affect women's rights and participation.
- The Global Digital Compact (GDC) process represents a new opportunity to establish international guidelines for rights-respecting AI governance. It stresses that international cooperation is required to promote coordination and compatibility of emerging AI governance frameworks. It also emphasises transparency, accountability and human rights due diligence. The GDC principles highlight the need for human rights assessments, with

particular attention to the rights of women in all their diversity and systematically, structurally marginalised sectors of diverse populations. It calls on digital technology companies and developers to respect international human rights standards and principles, including through the application of human rights due diligence and impact assessments throughout the technology life cycle. It also calls on them to be accountable for and take measures to mitigate and prevent abuses, and to provide access to effective remedy in line with the United Nations Guiding Principles on Business and Human Rights and other relevant frameworks.

- The EU AI Act aims to regulate AI systems based on their risk levels, and specific provisions address the use of AI in public procurement processes. The Act designates certain AI systems as high-risk, including those used in critical areas such as law enforcement, migration, healthcare, education and public administration. For procurement purposes, public authorities must ensure that the AI systems comply with the Act's requirements for high-risk systems, such as:
    - Risk management and mitigation
    - Transparency obligations
    - Robust documentation and record keeping
    - Human oversight mechanisms.
    - Providers of high-risk AI systems must also undergo conformity assessments to certify compliance with the Act.
    - States are prohibited from using AI for real-time remote biometric identification in public spaces, except under narrowly defined exceptions for law enforcement. Public bodies must conduct periodic evaluations of deployed AI systems to verify their continued compliance and effectiveness. States are encouraged to engage stakeholders and civil society organisations when deploying AI systems with a significant societal impact.
- The OECD Recommendation on Public Procurement provides a comprehensive framework for improving the efficiency, transparency and integrity of public procurement systems. It highlights key principles, including transparency (open processes and access to procurement information); accountability (clear oversight mechanisms and sanctions for violations); and integrity (measures to prevent corruption, fraud and conflicts of interest). The OECD AI Principles emphasise human-centric design; transparency and explainability; and robust risk assessment and mitigation mechanisms.

- The UNESCO Recommendation on the Ethics of AI calls for ethical principles that apply to AI procurement, including respect for human dignity and rights; fairness and non-discrimination; and accountability and transparency. The Recommendation provides for specific gender- and environment-related ethical concerns that could be applied to frame public procurement of AI.

4. Are there any emerging positive business practices that include human rights requirements when procuring and deploying AI? Please provide examples.

Some businesses have begun incorporating human rights assessments in AI procurement, though these remain limited. A key concern in this regard is technology-facilitated gender-based violence (TFGBV) and its consequences on both the digital and the analogue realm.

Companies deploying AI tools have the opportunity to incorporate proactive detection systems for online harassment and abuse, with specific attention to gendered patterns of violence. They can also strengthen user-centric reporting mechanisms that account for various forms of TFGBV. An emerging practice that can be enhanced and supported is the implementation of "safety by design" principles that consider TFGBV risks in AI deployment. Another emerging practice that deserves deeper consideration and wider adoption is the inclusion of TFGBV prevention measures in service level agreements and vendor contracts, as well as clear protocols for addressing identified instances of technology-facilitated violence and exclusion.

For these practices to be truly effective, they must be accompanied by substantial consultation with affected communities through all the stages of AI procurement and deployment, as well as regular evaluation of their impacts – intended and unintended.

5. How have businesses outside the technology sector included human rights impacts related to the procurement and deployment of AI systems in their human rights due diligence processes? Please provide examples.

From the perspective of communications and access to technology, current due diligence processes in non-technology businesses rarely address the intersectional impacts of AI systems adequately. The adoption of human rights due diligence processes for AI systems by businesses outside the technology sector represents a crucial opportunity to mainstream intersectional assessments across diverse industries. While some corporations have begun incorporating AI impact assessments into their human rights due diligence, these often fail to consider the compound effects of multiple forms of discrimination, particularly affecting women and girls, in all their diversity; more robust frameworks are needed that specifically examine how AI systems affect different marginalised groups across various contexts. Mainstreaming these practices requires sustained commitment to long-term investment in capacity and resources, alongside regular evaluation and adaptation of approaches.

As examples, financial services can examine AI-driven credit scoring impacts on women across socioeconomic backgrounds; healthcare can evaluate AI diagnostic tools' performance across diverse populations; and agricultural businesses can assess how AI farming technologies affect women farmers in different regions. Organisations are also beginning to recognise the necessity of comprehensive intersectional analysis in their AI deployment.

The potential for mainstreaming these practices lies in their systematic ability to address diverse women's needs, create scalable solutions adaptable across contexts, and generate evidence for the business case of inclusive AI deployment. This is being achieved through the development of sector-specific guidelines, creation of shared assessment tools, establishment of cross-sector learning platforms, and implementation of training programmes that build organisational capacity in gender-responsive technology evaluation.

Current practices demonstrate promising evolution through stakeholder engagement and documentation processes. Businesses can, and should, collaborate and consult with women's organisations and affected communities across different contexts, partnering with local experts who understand specific regional challenges, and creating case studies that highlight successful intersectional approaches.

6. How can businesses and states meaningfully engage with relevant stakeholders, including potentially affected rights holders and workers, to identify and address adverse human rights impacts related to the procurement and deployment of AI? Please provide examples.

Meaningful engagement between businesses, states and stakeholders in addressing AI-related human rights impacts requires a fundamental shift towards inclusive, participatory approaches that centre the experiences of women and girls in all their diversity. This engagement must recognise and actively work to overcome existing obstacles to participation, including digital divides, language barriers, accessibility issues and socioeconomic constraints that often prevent marginalised communities from contributing to discussions about AI procurement and deployment.

The development of effective consultation mechanisms needs careful consideration of the intersecting factors that constitute vulnerabilities, including gender, race, class, disability, geographic location and digital literacy. States and businesses must establish ongoing dialogue platforms that accommodate different levels of technical knowledge and provide appropriate resources for meaningful participation, including translation services, technical support and compensation for time and expertise. These platforms must prioritise engagement with grassroots organisations, women's rights groups and community leaders who can provide crucial insights into how AI systems impact various communities differently.

Furthermore, successful stakeholder engagement will require moving beyond traditional consultation models to establish genuine partnerships that influence decision-making processes throughout AI development and implementation. This includes involving affected communities in initial needs assessments, system design, testing phases, implementation, and ongoing monitoring and evaluation. States and businesses must create formal feedback mechanisms that ensure stakeholder input leads to concrete actions and changes in AI procurement and deployment practices, with particular attention to how these systems affect women and girls' access to services, economic opportunities and fundamental rights.

To mainstream these practices effectively, states and businesses will need to institutionalise intersectional approaches to stakeholder engagement through policy frameworks, dedicated resources and accountability mechanisms; this includes establishing complete and constantly updated guidelines for inclusive consultation processes, creating permanent channels for stakeholder input, and developing metrics to evaluate the effectiveness of engagement efforts. This institutionalisation must also be accompanied by capacity-building initiatives that enable both decision makers and rights holders (bridging the gap between them) to participate effectively in discussions about AI governance and human rights impacts, ensuring that technological advancement serves to enhance rather than diminish the rights and opportunities of diverse communities.

7. Are there any positive practices of businesses providing access to remedy when they have caused or contributed to adverse human rights impacts linked to the procurement of AI systems and their deployment across their activities, including through the establishment of operational-level grievance mechanisms? Please provide examples.

Current operational-level grievance mechanisms for AI-related harms remain inadequate. While some companies have established specialised AI ethics boards, these rarely provide meaningful remedies for affected individuals and communities. However, the emerging positive practices in providing remedy for AI-related human rights impacts, particularly concerning TFGBV, demonstrate a growing recognition of businesses' responsibility to address harm. Leading companies have developed multi-channel reporting mechanisms that account for various forms of technology-facilitated abuse, implementing user-friendly interfaces that allow survivors to document incidents while maintaining their privacy and safety.

These mechanisms often include options for emergency assistance, clear documentation processes, and support in multiple languages, recognising that TFGBV affects women and girls across diverse contexts and requires culturally sensitive responses.

Companies are increasingly adopting trauma-informed approaches to their grievance mechanisms, incorporating insights from women's rights organisations and survivors in their design and implementation. This includes establishing dedicated teams trained in handling TFGBV cases, providing multiple channels for reporting (including offline options for those with limited digital access), and ensuring that response protocols prioritise survivor safety and agency.

Effective remediation practices must demonstrate a commitment to transparency and accountability through regular public reporting on cases, clear timelines for response, and mechanisms for appealing decisions, as well as oversight committees that include external experts and affected community representatives, ensuring that remediation processes remain responsive to evolving forms of technology-facilitated violence. Businesses can, and should, collaborate and consult with women's organisations and affected communities to develop standardised frameworks that can be adapted across different contexts while maintaining sensitivity to local needs.

More promising practices include community-led oversight committees with actual decision-making power over AI deployment and modification. The potential for scaling these approaches lies in their ability to combine robust technical solutions with human-centred support systems, ensuring that remediation mechanisms address both immediate harm and underlying systemic issues that contribute to TFGBV.

8. Are there any positive practices related to state-based remedy mechanisms in relation to human rights impacts linked to the procurement and deployment of AI? Please provide examples.

State-based remedy mechanisms specifically addressing AI-related human rights impacts are still emerging. The evolution of these remedy mechanisms demonstrates a growing recognition that effective redress for AI-related harms requires both strong institutional frameworks and deep understanding of how technology intersects with existing patterns of discrimination and violence against women and marginalised communities. The potential for mainstreaming these positive practices lies in their ability to combine robust legal frameworks with practical support mechanisms and preventive measures.

State-based remedy mechanisms addressing AI-related human rights impacts are evolving to meet the complex challenges posed by TFGBV, discrimination and exclusion. Governments are increasingly sharing best practices through international networks, developing common standards for AI impact assessment and remediation, and collaborating on cross-border enforcement mechanisms. Some states have begun establishing specialised digital rights units within existing human rights institutions, equipping them with technical expertise and resources to handle complaints related to AI systems. However, these mechanisms often lack adequate resources and enforcement powers. For these units to be effective, they must work in conjunction with gender equality bodies and data protection authorities, creating integrated approaches that recognise the intersectional nature of AI-related harms and their disproportionate impact on women and marginalised communities.

Also, states have begun to develop legal frameworks that explicitly address algorithmic discrimination and technology-facilitated violence, providing clear pathways for affected individuals to seek redress. These frameworks must evolve to include provisions for collective complaints, recognising that AI-related harms often affect entire communities rather than just individuals, and incorporate mechanisms for expedited review in cases of urgent digital violence. States are also adopting practices to invest in capacity building for judicial officers, law enforcement and other relevant authorities to better understand and address TFGBV and algorithmic discrimination.

Some states have also established dedicated funds to support victims of TFGBV in accessing legal support and technical expertise, acknowledging that meaningful access to remedy requires both legal frameworks and practical support.

9. What state-based remedy mechanisms are available to victims in case of adverse human rights impacts linked to the procurement and deployment of AI systems by businesses and state entities? Are there any court cases or judgments that you are aware of related to the procurement or deployment of AI by the state or businesses and human rights implications? Please provide examples.

Current legal frameworks struggle to address AI-related human rights violations effectively. While some automated decision discrimination cases have been successfully pursued through existing human rights bodies such as the European Court of Human Rights,[2] and others at national and subnational levels,[3] the technical complexity of AI systems often presents significant barriers to justice. A crucial challenge lies in recognising the intersection of identities and the implications of compounded vulnerabilities with regard to human rights impacts, particularly in the case of women and girls in all their diversity.

[2] Szabó and Vissy v. Hungary (2016), which dealt with automated data collection and processing systems; see https://hudoc.echr.coe.int/fre?i=002-10821

[3] The Dutch Court of The Hague ruled in 2020 on the SyRI (System Risk Indication) case, finding that this algorithmic risk assessment system used to detect welfare fraud violated human rights; see https://digitalfreedomfund.org/the-syri-welfare-fraud-risk-scoring-algorithm; the French Constitutional Council ruled in 2020 on the use of algorithms for university admissions (Parcoursup platform); see https://www.conseil-constitutionnel.fr/en/decision/2020/2020834QPC.htm; the Supreme Court of Wisconsin (United States) ruled in 2016 in State v. Loomis regarding the use of algorithmic risk assessments in criminal sentencing; see https://harvardlawreview.org/print/vol-130/state-v-loomis

National human rights institutions, equality bodies and data protection authorities are increasingly developing expertise in handling AI-related complaints, with some jurisdictions establishing specialised tribunals or divisions focused on algorithmic harm. These mechanisms are particularly crucial for addressing TFGBV and algorithmic discrimination, as they often provide more accessible and specialised pathways for redress than traditional courts, including options for collective complaints and expedited procedures in cases of urgent digital violence.

Court cases challenging discriminatory AI systems are emerging globally, including challenges to automated decision-making systems in public services and issues of transparency, accountability and discriminatory impacts. Cases involving predictive policing algorithms, welfare benefit distribution systems, and automated hiring tools have highlighted how AI systems can perpetuate and amplify existing gender and racial biases.

These cases are establishing important precedents for holding both state entities and businesses accountable for AI-related human rights violations. This must include efforts to build technical capacity within judicial systems, establish clear chains of responsibility for AI-related harms, and create mechanisms for meaningful participation of affected communities in oversight processes.

10. Are there any state, business or CSO-led processes or systems to provide protection for human rights defenders that may be at risk and/or affected by AI systems procured and deployed by state entities or business enterprises? Please provide examples.

Civil society organisations (CSOs) and activists working on human rights in the digital age face complex challenges in developing protection mechanisms against AI-related threats, while often operating with limited resources and technical capacity. Protection mechanisms for human rights defenders addressing AI-related harms remain severely underdeveloped. While some civil society organisations have established digital security support networks, comprehensive protection frameworks specifically addressing AI-related threats to human rights defenders are largely absent.

Protection systems must constantly evolve to address emerging forms of surveillance, automated harassment, and digital threats that are increasingly sophisticated and difficult to detect. The rapid deployment of AI systems by both state entities and businesses creates additional burdens for CSOs, requiring them to simultaneously document violations, support affected defenders, and advocate for stronger safeguards.

The transnational nature of AI-related threats poses particular challenges for CSO-led protection mechanisms, requiring coordination across different jurisdictions and contexts. Organisations must navigate varying legal frameworks, cultural contexts and technical infrastructures while trying to provide consistent support to defenders at risk. The rapid pace of AI development and deployment also means that protection mechanisms can quickly become outdated, requiring constant adaptation and learning that many CSOs struggle to resource adequately.

Civil society organisations are increasingly working to formalise their protection protocols, develop replicable models for AI-related threat assessment and response, and build stronger networks for knowledge sharing and mutual support. Efforts are increasing to strengthen collaboration between technical experts, human rights organisations and affected communities. A constant challenge is developing protection mechanisms that remain responsive to evolving threats while addressing the specific needs of defenders working in different contexts.

Many CSOs struggle with the dual challenge of providing immediate protection while also working to address systemic issues related to AI deployment. Organisations must balance urgent response needs, such as supporting defenders facing immediate digital threats, with longer-term work to build collective understanding of AI-related risks and develop appropriate protection strategies. This work is further complicated by the opacity of many AI systems and the difficulty in attributing specific harms to particular deployments or entities.

Resource constraints significantly impact CSOs' ability to provide comprehensive protection mechanisms, particularly in Global South contexts where organisations may lack access to specialised technical expertise or tools for detecting and mitigating AI-related threats. The intersection of digital and physical security risks requires holistic protection approaches that many organisations struggle to fund and maintain. Additionally, CSOs often face their own security risks when documenting AI-related human rights violations or supporting targeted defenders.

11. Please provide any comments, suggestions or additional information that you consider relevant to this thematic report.

Future policy development must centre the experiences of those most affected by AI systems while building stronger accountability mechanisms for both states and businesses. A feminist and intersectional approach to AI governance is necessary and requires fundamental changes in how technology and rights are conceptualised; this includes moving beyond technical solutions to address underlying power structures, ensuring meaningful participation of women and systematically marginalised communities in AI governance, as well as developing new frameworks for updated and complete digital rights.